

REMARKS

Claim 21 has been amended for purposes of clarity only and thus for reasons unrelated to patentability.

Request for Examiner Interview.

Should the Examiner be of the opinion that this Amendment does not place the application in a condition for allowance, Applicant hereby requests an Examiner Interview prior to the issuance of the next communication from the USPTO to expedite prosecution.

The nonstatutory obviousness-type double patenting rejection of Claims 1-21 over Claims 1-30 of U.S. Pat. No. 7,228,563 has been obviated.

The Examiner states:

A timely filed terminal disclaimer ... would overcome an actual or provisional rejection on this ground provided the conflicting application or patent is shown to be commonly owner with this application. (Office Action, page 3.)

To expedite prosecution, co-filed herewith is a Terminal Disclaimer to Obviate a Double Patenting Rejection Over a "Prior" Patent (1 page) and a Statement Under 37 CFR 3.73(b) (1 page). The Terminal Disclaimer obviates the nonstatutory obviousness-type double patenting rejection of Claims 1-21 over Claims 1-30 of U.S. Pat. No. 7,228,563.

For at least the above reasons, Application respectfully requests reconsideration and withdrawal of this rejection.

Claims 1-21 are novel over Swimmer et al. (2004/0255163).

Regarding Claim 1, the Examiner states:

Swimmer teaches a method comprising: stalling a call to an operating system function **originating from a call module**; and determining whether **said call module**

is in a driver area of a kernel address space of a memory ... (Office Action, page 4, emphasis added.)

The Examiner's statement is respectfully traversed.

As set forth in MPEP § 2131, Eighth Edition, Rev. 5, Aug. 2006, at page 2100-67:

TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM

As demonstrated below, the Examiner has failed to callout where Swimmer et al. teaches every element of Claims 1-21. Accordingly, Claims 1-21 are allowable over Swimmer et al.

Swimmer et al. teaches that the system calls are from a user-mode program in a user-mode memory. Specifically, Swimmer et al. teaches:

Referring to FIGS. 2, 3, 4, and 5 together, in operation, the intrusion detection sensor 14 monitors system calls 44, 440 from a **user-mode program such as the daemon 12 executed in a user-mode memory 51** of the host computer 10 and forwarded to the operating system 11. (Paragraph [0043], emphasis added.)

Similarly, in the Summary of the Invention, Swimmer et al. teaches:

In a particularly preferred embodiment of the present invention, the sensor is adapted to: intercept system calls that are forwarded to an operating system from at least one daemon or similar program **executed from a user-mode memory** of a monitored host computer ... (Paragraph [0024], emphasis added.)

Further, Swimmer et al. teaches that a user-mode memory is different than a kernel mode memory:

... modern operating system architectures separate code executed by users, often called shellcode, from code executed by the operating system 11 to protect the core or kernel of the operating system 11 from damage caused by errant or malicious programs. To achieve this, modern processors include a mode bit that specifies

whether the processor is executing **kernel-mode code** or **user-mode code**. If the mode bit is set, meaning **user-code** is executing, then the processor prevents all access to **kernel memory spaces** such as the memory spaces 52, 53. However, because daemons utilise functionality provided by the operating system 11 to access disk drive drivers 305, network connection drivers 306, other drivers 307, and the like, those programs utilise system calls, that expose relevant functionality of the operating system 11 to **user-mode programs**. ... (Paragraph [0044], emphasis added.)

For at least the above reasons, Swimmer et al. does not teach or suggest:

A method comprising:
stalling a call to an operating system function **originating from a call module**; and
determining whether **said call module is in a driver area of a kernel address space** of a memory,

as recited in Claim 1, emphasis added. Accordingly, Claim 1 is allowable over Swimmer et al. Claims 2-17, which depend from Claim 1, are allowable for at least the same reasons as Claim 1. Claim 21 is allowable for reasons similar to Claim 1.

For similar reasons, Swimmer et al. does not teach or suggest:

A method comprising:
hooking driver load and unload functions;
obtaining loaded driver information;
determining **a driver area in a kernel address space of a memory**; and
determining whether a driver has been loaded into or unloaded from **said kernel address space**, wherein upon a determination that said driver has been loaded into or unloaded from **said kernel address space**, said method further comprising **updating said driver area**,

as recited in Claim 18, emphasis added. Accordingly, Claim 18 is allowable over Swimmer et al. Claims 19-20, which depend from Claim 18, are allowable for at least the same reasons as Claim 18.

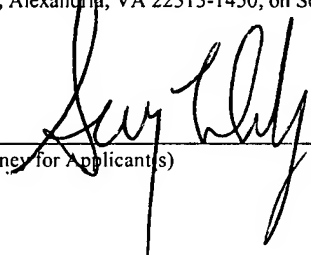
For the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

Conclusion.

Claims 1-21 are pending in the application. For the foregoing reasons, Applicant respectfully requests allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF MAILING

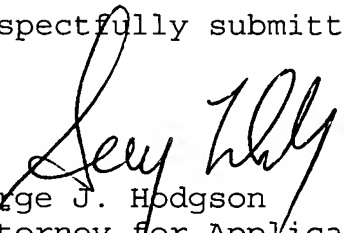
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on September 28, 2007.



Attorney for Applicant(s)

September 28, 2007
Date of Signature

Respectfully submitted,


Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880